Issue 2
March 2004

IT Security – The New Technology Gold Rush

Clarity Brief

# IT Security – The New Technology Gold Rush

Written By Eric Shuster
President and CEO of IntelliClear – March 2004

Beyond death, taxes, and a new Microsoft Windows patch, one thing that can be counted on like clockwork is the evolution of information technology (IT). With each new IT evolution comes a fresh opportunity for innovation, integration, and incremental revenues for all those in the IT value chain. As history has shown, such opportunities are perishable and highly competitive. One cannot help but liken these opportunities to the gold rush of 1849, where over 200,000 gold seekers converged on California from all over the world to seek their fortune. The IT market has historically spawned one gold rush after another, each one delivering its share of winners and losers. The latest gold rush in the technology sector is IT security. Using a variety of data from numerous independent sources, IntelliClear takes a brief, yet comprehensive look at the IT security space to unfold the market opportunity, the drivers of demand, the players that are poised to cash in, and a glimpse of what the future may hold for this hotter than hot space.

ABSTACT:
IT security is a red hot area in the IT industry and is generating interest world wide among large, medium, and small companies. Fueled by global fears, increased regulation, SPAM, and regular virus outbreaks, companies are scrambling to secure their IT infrastructures like never before. Suppliers of IT products and services including IT security companies, OEMs, networking manufacturers and channel partners, are rushing to supply the demand, while others outside of IT like banking and employment agencies stand to cash in as well. The result will be dramatic increases in spending and opportunities for a wide range of industries and trades. Indeed, IT security is the new technology gold rush.

IntelliClear
Bringing Clarity to IT Market Intelligence
Clarity Brief

**Security Then, Security Now:**

Man has been dealing with information security issues since the earliest days when secret messages were sent from one individual to another, with various forms of confirmation and authentication. RSA's e-security Experience presentation from their website http://www.rsasecurity.com/experience/esecurity/#, provides a clever example using Roman soldiers sending confidential messages with wax seals from city to city, authenticated and authorized in various ways, complete with non-repudiation processes. The RSA presentation outlines the progression of security from manual cryptography, to mechanized cryptography, to the computerized cryptography of the present day. Such a suggestion provides a strong historical perspective for today's sophisticated IT security solutions and replaces the notion of such solutions being web-based sci-fi, to their being the natural evolution of information security.

**The mission of the Information Security department is to protect the information assets, the information systems, and network that deliver the information, from damage resulting from failures of confidentiality, integrity, and availability.**

The team at IntelliClear considered providing a simplified diagram of what a typical IT security infrastructure would look like today, identifying components and concepts to provide a solid footing for the remainder of the paper. However, upon attempting to do so it became quickly evident that IT security has become an enormously complex and specialized technology, with innumerable varieties of configurations and choices, that such a diagram would do little to enlighten the reader.

Such a diagram would depend on the existing IT infrastructure, the security objectives of the organization, a given budget, and the recommendations of the individual or firm designing the solution. In its most theoretical form, Ken Shaurette described the mission of most IT security organizations to be the following:

> *The mission of the Information Security department is to protect the information assets, the information systems, and network that deliver the information, from damage resulting from failures of confidentiality, integrity, and availability (CIA).*[1]

The mission is to protect the ecosystem from failures of "CIA". To accomplish this mission, IT security departments of today will utilize an arsenal of hardware and software technology to address and fortify the triad of confidentiality, integrity, and availability.

The solutions deployed will address and utilize such components as authentication, content filtering, digital certificates, encryption, firewalls, Internet Protocol Security (IPsec), intrusion detection, Kerberos, public key encryption, S/MIME, network sniffers, secure electronic transactions, Secured Socket Layer (SSL), single sign-on, and virtual private networks (VPN) – to name a few. If this vocabulary appears strange to you, then you have a great deal of homework to do if you want to be a part of the new technology gold rush in IT security. If you don't speak or understand the language, the opportunity will likely pass you by. There are numerous glossaries, books, magazine articles, websites, consultants, VARs, and a host of industry experts who are ready to accommodate your education.

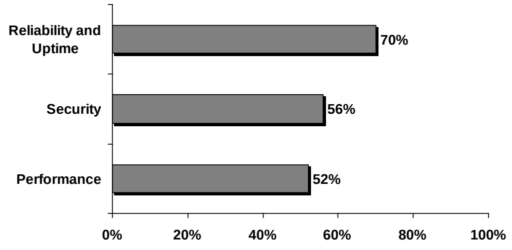
**IDC estimates that world wide (WW) IT security spending will reach $45 billion by 2006.**

**<u>How Hot is IT Security?</u>**

IDC estimates that worldwide (WW) IT security spending will reach $45 billion by 2006[2]. This number includes hardware, software, and services associated with IT security deployments across the globe. Security as a percentage of IT budgets across the world has skyrocketed to an estimated 8.2% according to the META group. META projects a 156% increase in WW spending from 2001 to 2003 on IT security as a percentage of the IT budget in 2003[3]. This spending is not isolated to large enterprises alone. AMI-Partners reported spending of $1.8 billion in 2003 on IT security solutions among US small and medium sized businesses (1-999 employees)[4], while INPUT estimates that US Federal Government spending on IT security reached $4.2 billion in 2003[5]. The IT security arm is reaching a multitude of markets.

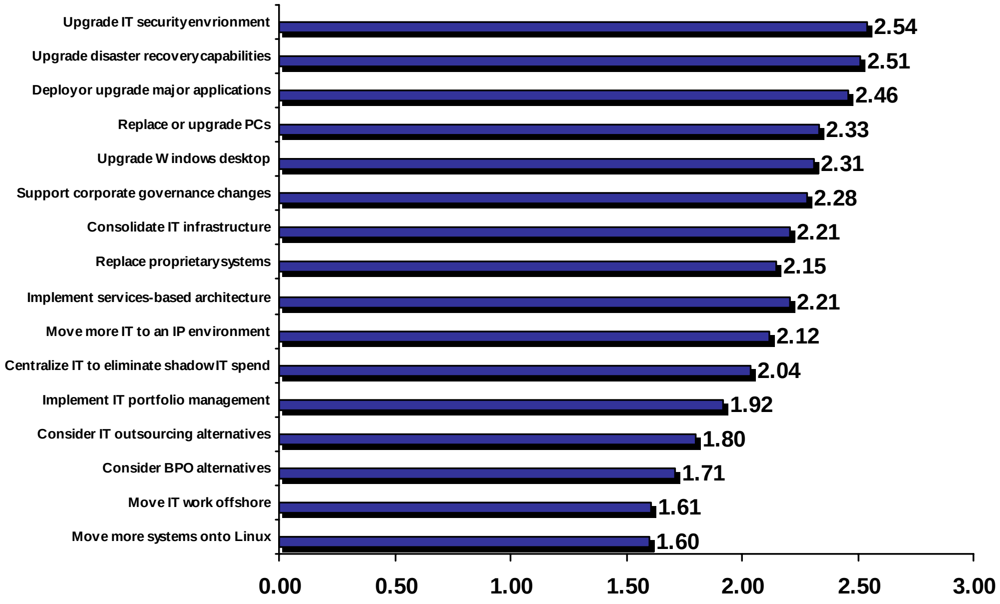
The importance of IT security cannot be measured solely by the money being spent to deploy solutions. Although significant and on a steep trajectory, spending alone does not tell the whole story. In a study of 280 WW IT Executives of large companies in March of 2003, IDC reported that 56% cited security as being their top concern, preceded only by reliability and uptime at 70%.[6] Such data collaborates with studies conducted by professional services magnate Deloitte & Touché, who reported IT security as being number 3 on a list of global CIOs top priorities[7], and Forrester Research who reported upgrading the IT security environment as being the number one priority of IT executives in North America according to a study in November of 2003[8].

**Top 3 Concerns Regarding IT among Business Executives Worldwide (as a % of respondents)**



Source: International Data Corporation (IDC), March 2003; n=280

**North American IT Executives' Leading IT Initiatives for 2004 (by average Index* score)**



**Source: Forrester Research, November 2003**
**NOTE: n=818 IT decision makers**
***where 1=not on agenda, and 4=critical in 2004**

**Businesses of all sizes are "putting their money where their mouth is" and catapulting security to the forefront of the IT opportunity landscape.**

Once again noting that these trends are not reserved for large enterprises along, nearly 50% of medium sized businesses (100-999 employees) identified 'building or maintaining up to date security and privacy policies" as the leading IT spending priority in 2003 according to ARC[9]. A similar result is seen among small businesses (1-99 employees), where nearly 1.9 million small businesses plan to "enhance their IT security by adopting higher-end solutions" according to an AMI study conducted in 2003.[10]

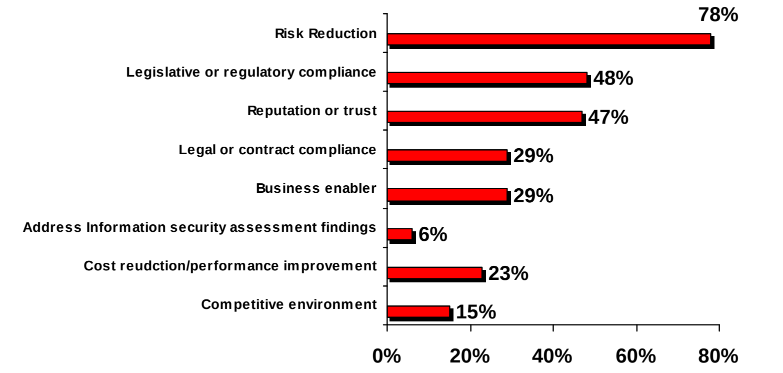
Data from these and many others studies on IT security attitudes, collaborates with the spending data, to confirm that businesses of all sizes are "putting their money where their mouth is" and catapulting security to the forefront of the IT opportunity landscape. Such commitments have created a "perfect storm" of activity around IT security, thus creating an enormous market opportunity for a wide variety of manufacturers and service providers of IT products and services – not just those that specialize in IT security.

## Drivers and Obstacles to IT Security:

Since businesses are making the deployment of IT security solutions a top priority, and budgeting significant capital to make those deployments happen, there must be a set of compelling drivers that are motivating this level of commitment. IntelliClear found that the majority of the motivation is being fueled by regulatory compliance, SPAM prevention and a desire to reduce the risks associated with process improvements and business operations that are becoming more Internet centric. Accounting firm Ernst & Young, working with world wide IT executives, found that risk reduction, legislative and regulatory compliance, and the protection of corporate reputation and trust were the key drivers of IT security implementations.[11] While corporate compliance and risk mitigation act as IT security drivers, the threat of intellectual property theft, malicious code, and financial fraud are seen as posing the greatest threats to the business of large enterprises according to Forrester Research.[12] These threats are powerful, as they appeal to the "emotional side" of executives and create powerful internal drivers that trickle down organizational structures.

**IntelliClear found that the majority of the motivation is being fueled by regulatory compliance, SPAM prevention and a desire to reduce the risks associated with process improvements and business operations that are becoming more Internet centric.**

**Factors that Are Most Influential in Driving Adoption of New Information Security Solutions Worldwide (as a % of respondents)**



Source: Ernst & Young, August 2003
NOTE: n=1,424 IT executives, multiple responses allowed

Some of the most prominent regulations driving IT security to the forefront are the following:

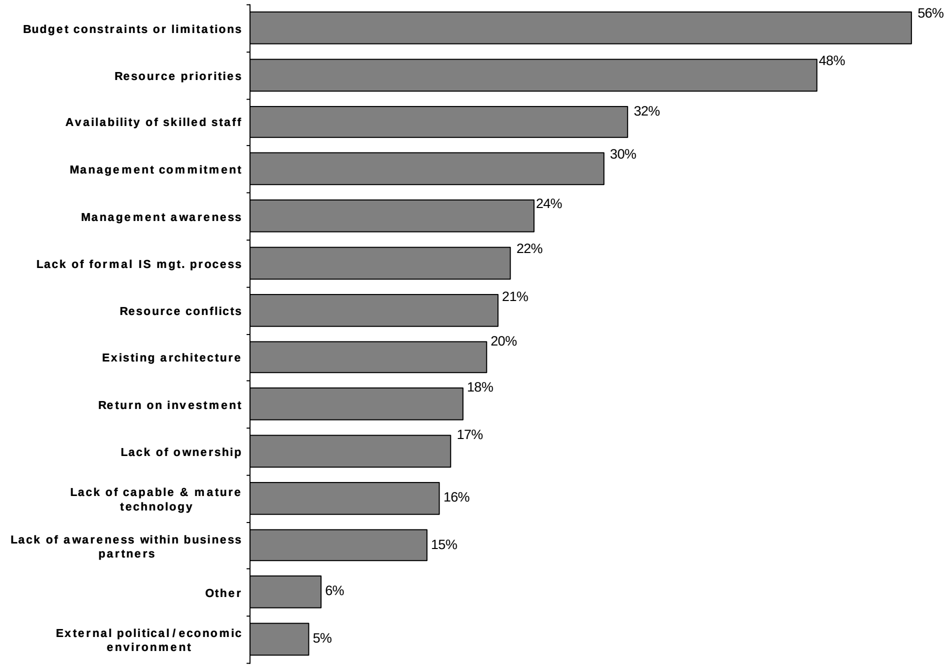
- Gramm-Leach Bililey Act: dealing with issues surrounding consumer financial information
- Sarbanes-Oxley Act of 2002: dealing with issues surrounding record keeping
- USA Patriot Act: dealing with issues pertaining to anti-terrorism
- North American Electric Reliability Council: concerned with the security of physical assets
- HIPPA: dealing with issues surrounding the security of patient information
- ISA 17799: dealing with certification requirements for securing information and information systems

To give one an understanding of how legislative policies can create business opportunities for IT product and service providers, consider an AMR study which reported that an estimated $2.5 billion will be spent to come into compliance with the Sarbanes-Oxley Act alone in 2003 and 2004.[13] Such regulations compel organizations to make investments into consulting to understand how to comply; software for monitoring data and associated activities; storage systems to archive data, identity management systems to regulate access; firewalls to keep out intruders; and the list goes on. These opportunities will range from working with large enterprises in the medical services industry, to brokerage firms who are challenged with instant messaging, to local schools who struggle with trying to comply with the recently passed Children’s Internet Protection Act.

**An AMR study reported that an estimated $2.5 billion will be spent to come into compliance with Sarbanes-Oxley Act alone in 2003 and 2004.**

While there are plenty of reasons why IT managers should invest in securing their respective infrastructures, there are two strong obstacles that are true barriers to striking gold in the IT security space:  money and resources. 56% of world wide IT executives cited budget constraints or limitations as the key obstacle to security investment, while 48% are hampered by resource priorities and/or lack of skilled staff according to Ernst & Young. [14]  Both are difficult to overcome, leaving many companies with sub-standard IT security infrastructures and policies.

**Significant Obstacles to Effective Information Security Worldwide (as a % of respondents)**



Source:  Ernst & Young, August 2003; n=1,413 IT executives, multiple responses allowed

IntelliClear strongly suggests that vendors and executives focus on taking the time to develop strong IT security return on investment (ROI) scenarios for management, thus helping them to clearly understand the nature of the investment and what will be gained in the short and long run. CIO Insight reported in March of 2003 that only 29.2% of US CIOs formally calculated ROI for security/identity management investments.[15] Citing the aforementioned Ernst & Young study, although only 18% of world wide IT executives claim ROI is an obstacle to IT security, IntelliClear believes well executed ROI portfolios can help address the issues identified relating to lack of management commitment and awareness of IT security. Greg Shipley of *Network Computing* suggests "calculating the annualized loss expectancy (ALE) using asset values, the percentage of loss expected per incident, and the total number of estimated incidents. By determining the ALE, you could compare it to the costs of maintaining the IDS solution (essentially, IDS' TCO), which could then be used to calculate the technology's ROI.[16] Well thought-out, creative, and legitimate methods of ROI calculation will help bolster security investment justifications and help pave the way for IT security deployments.

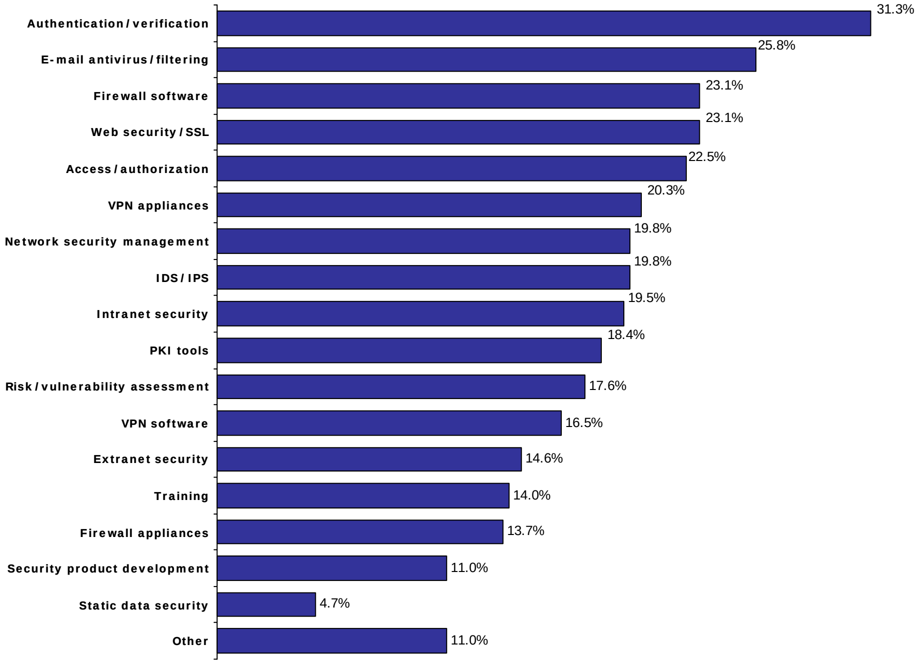
**Well thought-out, creative, and legitimate methods of ROI calculation will help bolster security investment justifications and help make available the required dollars for IT security deployments.**

**Hottest Areas of Security:**

Beyond the critical drivers of IT security are the specific solutions that are creating the greatest opportunities. Starting from the top down, IT security technology (hardware and software) tops the list of spending categories for WW IT executives, followed by business continuity solutions and process solutions.[17] IT security technology can be broken down into several different categories. IntelliClear examined a number of studies which attempted to identify the most critical splits and found various discrepancies, leaving room for debate and interpretation. One such study we examined came from the Emmes Group which identified the most immediate needs among IT professionals with respect to enhancing computer/network security to be authentication/verification, email antivirus/filtering, firewall software, web security/SSL, and access/authorization.[18] A study from Aladdin Knowledge Systems on security technologies found that WW IT professionals were currently evaluating anti-spam, antivirus, intrusion detection, and firewalls more than any other IT security technologies.[19] For small businesses the focus is more on antivirus, firewalls, and data back up. One driver in the wings that will certainly have an impact will be wireless LAN, which is poised to continue substantial growth, amid a host of security concerns.

**Starting from the top down, IT security technology (hardware and software) tops the list of spending categories for world wide IT executives, followed by business continuity solutions and process solutions.**

**Most Immediate Needs with Respect to Enhanced Computer/Network Security according to IT Professionals in the US (as a % of respondents)**

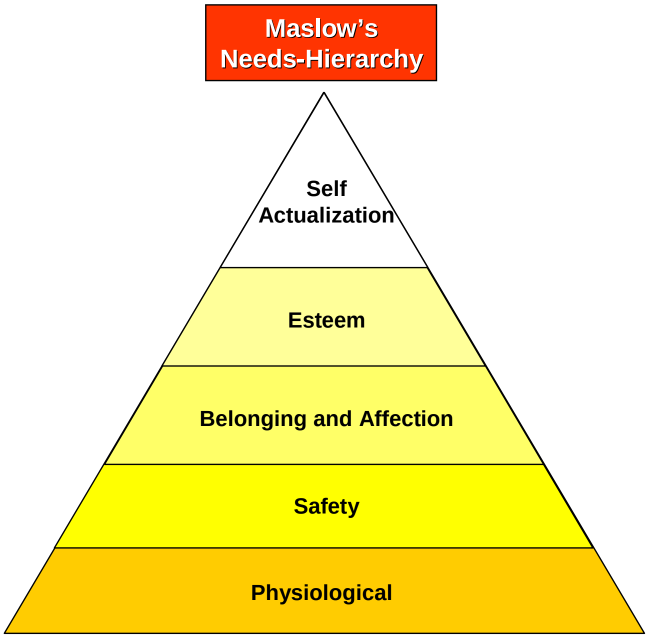


**Source: Emmes Group for Stonesoft, May 2003; n=375 RSA 2003 conference attendees**

To better understand the IT security attitudinal and behavioral dynamics across companies of all sizes, IntelliClear has developed the IT Security Needs Hierarchy, patterned after the conceptual model of Abraham Maslow who developed the Human Needs Hierarchy model in the 1940's. Maslow theorized that humans will first seek to meet their most important needs first, starting at the most basic.

The model begins with the fulfillment of physiological needs, such as hunger, thirst, and other basic need. Once physiological needs are meet, humans then see to meet needs surrounding safety such as shelter and protection from harm. Once the need for safety is obtained, Maslow then theorized that humans act to fulfill their needs for belonging and affection (love). The next stage in the model is the need for esteem including self-esteem, respect, and recognition. The final stage in Maslow's model that humans seek to fulfill is the need for self-actualization, which would include such things as self-fulfillment and job satisfaction. Fulfillment of each level is sequential in nature, suggesting an intrinsic need to satisfy the most important needs first before moving forward. Maslow's Needs-Hierarchy framework is a classic model in human behavior.

**IntelliClear believes this same pattern of needs fulfillment exists with IT security.**



Source: Abraham Maslow, 1908 - 1970

IntelliClear believes this same pattern of needs fulfillment exists with IT security. At the lowest level, akin to the physiological level, are virus protection/back-up/and policies. These are the easiest components to understand and deploy for a business, with each revolving around the tool most commonly found in nearly all commercial businesses – the PC. It should be noted that data back-up, although a foundational element, is often overlooked by even mid-sized companies.

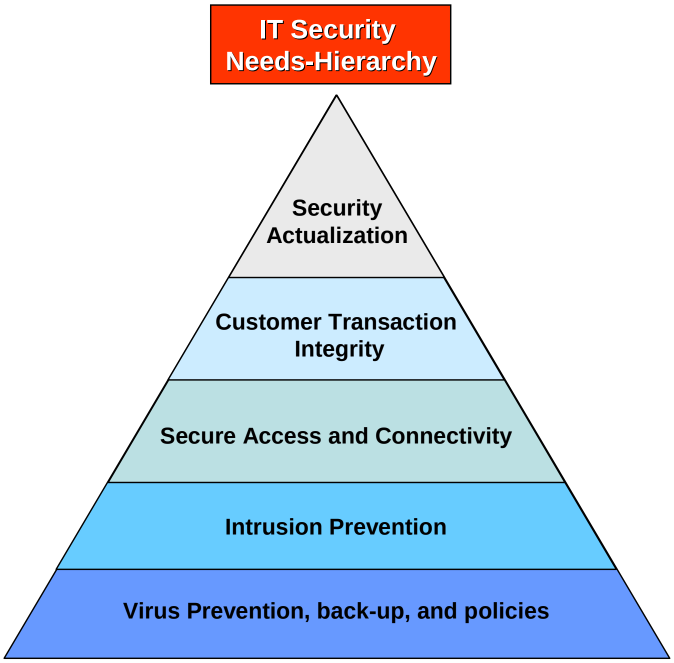
After securing stand-alone PCs and data, attention is then given to keeping the “bad guys” out by deploying *intrusion prevention* technology such as firewalls. This can be compared to the ability of a person being able to securely lock the doors of their home at night and feel relatively safe in doing so. Broadband and LAN server usage are typically strong catalysts to entering this level of the IT security Needs-Hierarchy model.

After securing the perimeter of the company, businesses are likely to establish *secured access and connectivity* in and out of their IT infrastructure via authentication and VPN solutions. Deployment may include strong authentication methodologies and digital certificates as appropriate and required. Successful deployment of this stage will allow businesses to communicate from the outside in with as little anxiety and risk as possible.

**Upon successfully achieving secured access for internal employees, attention is likely to be turned to the next level of IT security – customer transaction integrity.**

Upon successfully achieving secured access for internal employees, attention is likely to be turned to the next level of IT security – *customer transaction integrity*. This level will allow customers to access company information and perform secured transactions within the firewall of the company. This functionality will call for layers of security including such technologies such as SET and SSL (Secure Socket Layer).

The final level, and highest level, of the IT security Needs- Hierarchy model is described as *security actualization*. At this point the company's fortress is protected with secured internal access and interactive customer transaction capability has been successfully deployed. At this final level of the IT security needs-hierarchy model security technology has been deployed that focuses on usability and creates optimal accountability across the virtual matrix of all inhabitants of the security ecosystem. Nirvana like technology and processes are deployed such as password synchronization or single sign-on, biometrics, secured wireless networks, highly effective SPAM filtering, and multi-level monitoring. Accountability is ensured, while the fortress begins to operate in a more relaxed mode where productivity is enhanced, yet security is maintained.


IT Security Needs-Hierarchy
Security Actualization
Customer Transaction Integrity
Secure Access and Connectivity
Intrusion Prevention
Virus Prevention, back-up, and policies

**Source: IntelliClear, 2004**

**Spending on security begets other IT spending, and residual opportunities come about as a result.**

**Established Security Players Opportunity:**

As quoted earlier, it is estimated that IT security spending, relating to hardware, software, and services, is expected to reach $45 billion by 2006. A large portion of this opportunity in the new technology gold rush belongs to the thriving pack of security focused technology vendors of today. These are firms who were once on the outskirts of IT technology, who survived the Internet crash, and established strong positions for their products and services in a recovering global economy. The leaders in this space include such leaders as Check Point, Computer Associates, Entrust, NetScreen, Network Associates, RSA Security, SonicWALL, Symantec, Trend Micro, VeriSign, and Watchguard Technologies. The opportunity for these best-in-class IT security players is clear, with each having staked out a respective position to sell products and services to large, medium, and small companies alike, even consumers. The opportunity here is bigger than just the purchase of a firewall or VPN. Generally speaking, spending on IT security solutions drives spending in other areas and creates new opportunities for IT vendors. Consider the following table from the Gartner Group, relating to the costs to set up a VPN:

**Cost Breakdown of Virtual Private Network**

| | |
|---|---:|
| Salaries to set up VPN | $75,000 |
| Larger Internet access pipe for HQ | $24,000 |
| VPN hardware and software | $8,300 |
| Client firewalls | $37,000 |
| End-user access charges (i.e. model/DSL) | $75,000 |
| ISP charges for end-user access | $60,000 |
| **Total:** | **$279,300** |

**Source: Gartner Group, 2000**

Although the data in the chart is from the year 2000 (the numbers may need a little updating), Gartner makes the point that the installation of one security solution can spawn spending across a number of different IT vendors, trades, and individuals.

A key theme for the IT security space in the next 12 to 24 months is consolidation. Consolidation has been happening in the IT industry since its inception and has heated up in the security space in the last year. Consolidation in the IT security space will happen on two fronts: 1) core IT security players merging or acquiring other core IT security players; and 2) non-core IT security players acquiring core IT security players.

An example of the first consolidation (core IT security player acquiring another core IT security player) would be the recent Check Point acquisition of Zone Labs for $205 million in cash and stock. Through this acquisition Check Point hopes to provide complete end-to-end security solutions and expand its presence among small and medium sized companies. It is reported that Check Point will announce a new product in the second quarter of 2004 that is described as an SSL VPN that will provide integrated authentication and content verification. These types of mergers will continue, especially as hardware and software integration continues to be sought after by customers seeking security solutions.

**NetScreen is coming to market with a new appliance that integrates a firewall, VPN, and intrusion detection into one device, a product that Juniper's channel will be well positioned to sell.**

An example of the second type of consolidation (non core-IT security players acquiring core IT security players) would be the recent acquisition of NetScreen by Juniper Networks. The deal, worth an estimated $4 billion in stock, will bring together a networking giant in Juniper, with a security giant in NetScreen – a marriage that would seem to make all of the sense in the world. Networking vendors are the in the strongest position to take advantage of vertical integration in relation to adding IT security to their portfolio of products and services (which Cisco did long ago). NetScreen is coming to market with a new appliance that integrates a firewall, VPN, and intrusion detection into one device - a product that Juniper's channel will be well positioned to sell. In this instance, where channel partners once had to integrate Juniper networking solutions with complimentary security offerings, now they can get it all from one vendor. Look for more of these types of acquisitions to happen among networking, PC, and software companies in the near future.

**<u>PC and Server OEM Opportunity:</u>**

A key group of miners in the new technology gold rush are the PC and server OEMs. By PC and server OEM we refer to companies such as Dell, Gateway, HP, IBM, Sony, and Toshiba. These OEMs provide such key components of the infrastructure as PC clients, servers, and storage. PC and Server OEMs have been poking at IT security since pre-installing anti-virus software on PCs many years ago. Such efforts evolved into remote manageability, which included the integration of intelligent manageability code into ASICS to provide high level monitoring for IT administrators.

Servers have long included software components, redundancy, and other technology features to address various IT security concerns. IBM's On-demand initiative includes key communication messages on how security can be enhanced via its new revolution of bandwidth allocation. Intel corporation, a key supplier to the OEMs, has been extremely active in the security arena with 64-bit computing and the intelligent platform management interface (IPMI - New authentication and encryption algorithms that enhance security for remote management access). Intel has been a driving force of the trusted computing group (TCG), which is focused on specifying an important piece of an overall security solution - a hardware chip known as the Trusted Platform Module (TPM). The TCG is currently comprised of a variety of vendors, including PC platform, operating systems, and TPM vendors, with the board of directors consisting of representatives from Intel, IBM, HP, Microsoft, Sony, Sun Microsystems, Seagate, Verisign, and AMD. TPM vendors include Atmel, Infineon, National Semiconductor, and STMicroelectronics.

**From a revenue perspective IT security has helped drive the sales of PCs and servers, helping OEMs capitalize on the IT security theme.**

From a revenue perspective IT security has helped drive the sales of PCs and servers, allowing OEMs to capitalize on the IT security theme. Some OEMs have been offering various security products and services, but have stayed clear from committing large sums of capital to procuring sophisticated IT security solutions. Security issues will continue to drive the need for more secure PCs and bigger and stronger servers. For OEMs to drive even higher levels incremental revenue in the new technology gold rush they will need to think outside of their comfort zone to come up with simple ideas and useful innovation on IT security to deliver value and utility to customers.

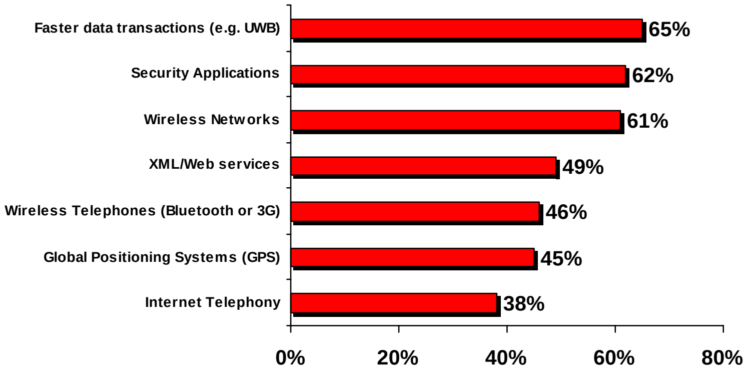
For example, a study conducted by Pointsec Mobile in July of 2003 found that 33% of PDA users in the US were storing their password/PIN information on their PDAs.[20] In April of the same year, SearchSecurity.com conducted a study among IT professionals in the US, Europe, and Asia, that found 75% were requiring their users to change network passwords three or more times per year, and that 44% wrote their passwords down in fear of forgetfulness.[21] If we put these studies together, we find users keeping their passwords on PDAs, and IT managers getting nervous about users writing their passwords down. As an OEM, why not leverage these findings and come up with a solution that utilizes the PDA as the password repository, while using wireless Bluetooth technology for input to the client PC on the network? Such a solution may help sell PDAs, while enhancing security to the enterprise.

PC OEMs may also begin to experiment more with offering a variety of security products with their line-ups, either as bundles or add-ons. VARBusiness reported in August of 2003 that 15.1% of US medium businesses are expected to deploy Biometric security devices. [22] These devices will offer “off-the-shelf” opportunities for incremental OEM revenue.

**PricewaterhouseCoopers reported in April of 2003 that 61% of CEO’s at the fastest growing US companies expect to see strong WLAN developments in the enterprise.**

Another area of opportunity for OEMs will be in the wireless LAN (WLAN) space. PricewaterhouseCoopers reported in April of 2003 that 61% of CEO’s at the fastest growing US companies expect to see strong WLAN developments in the enterprise. WLAN was sandwiched between security applications at 62%, and XML/Web services at 49%. [23] When considering these findings in a broader light, there appears to be a real opportunity brewing for secure mobile wireless access to corporate databases and LANs. [24]

**Areas in Which CEOs at the Fastest-Growing US Companies Expect IT Developments over the Next Two to Three Years (as a % of respondents)**



Source: PricewaterhouseCoopers (PwC), April 2003

Offering “embedded WLAN functionality on notebooks” gives OEMs opportunities for higher average unit prices and creates additional opportunities for add on service and accessory sales such as hot spot subscriptions and notebook security devices. OEMs have picked up on this, driving the percentage of embedded WLAN on notebooks WW to an estimated 24% according to Strategy Analytics.[25] WLAN means big business for others down the value chain such as public establishments (Starbucks, McDonalds, airports, etc) and service providers – all of whom will need to deploy IT security solutions with their WLAN installations.

There are numerous opportunities for OEMs to tap into as it relates to IT security, both directly and indirectly, in order to cash in on this new technology gold rush.

### Networking Equipment Manufacturers Opportunity:

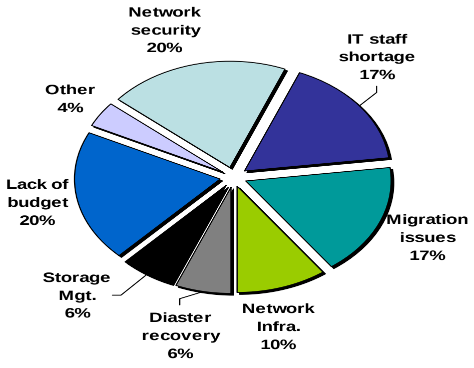
In moving closer to the heart of the IT security infrastructure we find the networking equipment manufacturers. Networking equipment manufacturers have been making money on IT security for many years, but in the last 12-24 months the opportunities have become even greater as the gold rush charges on. These opportunities range from revenues from the direct sales of security solutions, to the embedding of enhanced security on networking products, to partnerships that create synergy between networking products and security solutions.

**Network security was the number one concern among world wide IT administrators according to a study conducted by the Yankee Group in April of 2003.**

Cisco, the world's leader in networking products, and one of the chief innovators in the history of IT security, has been thinking security since it first started moving packets in the mid 1980's. Cisco's PIX firewalls are a favorite among IT professionals and only one of the many integrated product offerings that demonstrate a strong level of vertical integration as it relates to IT security. Juniper Networks has likewise made the commitment to vertical integration via NetScreen. IntelliClear expects to see more such acquisitions as networking manufacturers taking advantage of their close proximity to the core of the IT security infrastructure.

IT security issues will drive incremental network investments among companies of all sizes. Network security was the number one concern among WW IT administrators according to a study conducted by the Yankee Group in April of 2003.[26] Concerns over such critical issues as intrusion and data integrity are likely to lead to new investments in networking infrastructure. The Software Information and Industry Association (SIIA) reported in October of 2003 that 11% of North American IT professionals felt that improving the security of information was the most important driver of new network investments, second only to increasing network performance at 32%.[27] Morgan Stanley reported a similar finding among US CIOs in July of 2003.[28] Networking equipment manufacturers can expect to benefit from the gold rush through new investments in networking infrastructure as enhanced security solutions are deployed.

**Top Concerns for IT Administrators Worldwide
(as a % of respondents**



Source: Yankee Group/Sunbelt Software Inc., April 2003; n=1,000

Reversing the roles a bit: an area of networking growth that will drive security investments is the red hot wireless LAN (WLAN) space. Gartner Dataquest estimates that world wide WLAN shipments will reach 38.2 million units in 2004 among both businesses and consumers.[29] Morgan Stanley estimates that the year over year increase in WLAN spending from 2002 to 2003 to be 74%, the highest among all networking components.[30] The effect of these anticipated WLAN investments will be an increase in IT security investments, as security is a critical concern when it comes to WLAN. Organizations are expected to use Wi-Fi protected access (WPA), extensible authentication protocol (EAP), and WEP as the primary security methods for WLAN. [31]

**A CIO Tech Poll in December of 2003 revealed that 58% of IT executives planned to increase spending on security SW over the next 12 months.**

**Software Opportunities:**

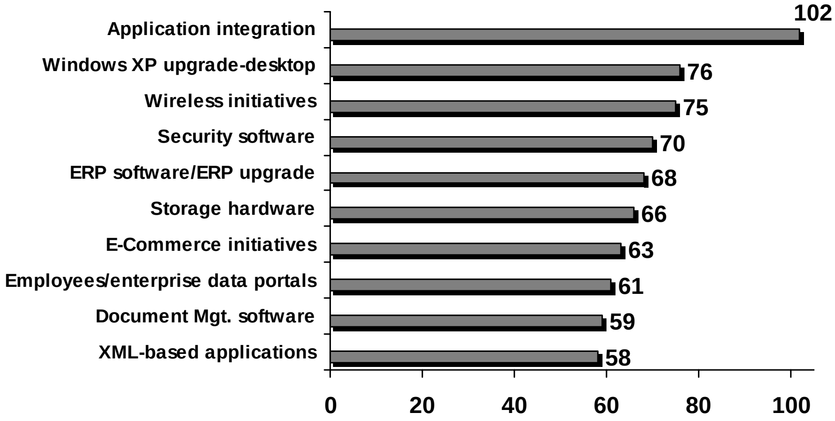
Hardware isn't the only benefactor of the new technology gold rush. IT security is having a dramatic affect on software opportunities – both vertical and horizontal alike. Whether it's the latest security patch from Microsoft, the acquisition of PowerQuest and ON Technology by Symantec, or the huge opportunity of performing custom software integration, IT security has given software another dimension to address and leverage.

A CIO Tech Poll in December of 2003 revealed that 58% of IT executives planned to increase spending on security SW over the next 12 months.[32] This spending is expected to be in addition to that being spent on software firewalls (i.e. Check Point), which when compared to hardware firewall appliances, creates quite a debate. Software firewalls are customizable, integratable to the O/S, deliver multiple platform support, and provide a level of hardware flexibility. Hardware firewalls on the other hand are plug-and-play, typically have lower initial costs, provide simplicity of administration, and have integrated security software. At the end of the day, there is a need for both types of firewalls depending on the particular application.

A critical area of software that is expected to dramatically increase as a result of the gold rush is custom integration - mainly via web service applications. PricewaterhouseCoopers reported in April of 2003 that CEO's of the fastest growing IS companies expect security applications (62%) and XML (49%) to be the key IT developments over the next 2-3 years. [33] Morgan Stanley reinforces that finding in July of 2003 when it found that application integration, security software, and XML were among the top IT priorities of US CIOs. [34] These application elements are expected to be at the center of e-business, CRM, and SCM deployments, helping to secure IP transaction processing and allow the realization of "IT security actualization" spoken of earlier.

**IntelliClear expects application integration efforts to generate sizable investments of capital into the IT security space, mainly among solutions providers and independent software vendors (ISV).**

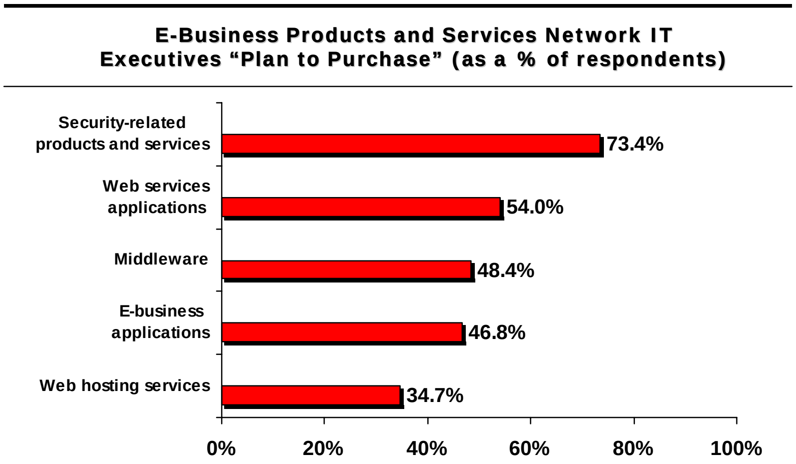
**Top 10 IT Priorities among US CIOs (In number of respondents)**



Source: Morgan Stanley, July 2003; n=225

IntelliClear expects these integration efforts to generate sizable investments of capital into the IT security space, mainly among solutions providers and independent software vendors (ISV). Network World reported in June of 2003 that the purchase plans of web service applications was second only to the purchase plans of security-related products and services among network IT executives. The same study revealed that security software, application components, and relational database/XML were ranked 1, 2, and 3 among the e-business products and services that IT executives were planning to purchase in the next 12 months. [35] Web services are self-contained, self-descriptive modular applications that can be located, published, and invoked across the Web. These applications/services can perform functions that range from simple requests to more complex business processes. Web services are typically distributed across many departments, or even companies. Web services are designed to allow different types of processes to act together and use the same data in a standard manner. On-going standards development will ensure basic interoperability of the common security infrastructure for web services.

As powerful as web services are, and as valuable as they can be to an organization, securing and protecting such broad, dynamic and “wide-open” environments has presented a tremendous security challenge. This challenge will provide opportunities for systems integrators, large and small, as well as established IT security vendors. OEMs such as IBM have already made great in-roads into positioning themselves as integrators for web services projects, as have Microsoft, Oracle, and SAP. Web services are still in their infancy as a technology, and as it grows the opportunities for IT security will grow along with it.

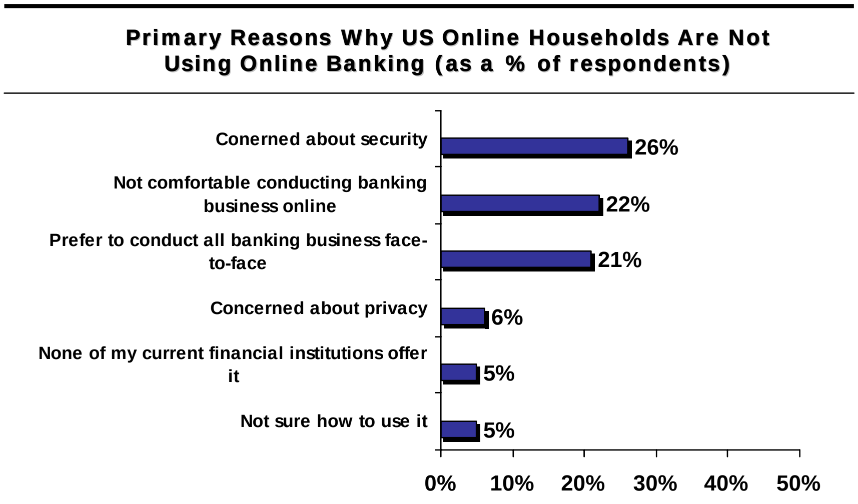


Source: Network World/Research Concepts, LLS, June 2003 (multiple responses allowed)

**The TowerGroup reported in June of 2003 that security was the primary concern of households as to why they were not using on-line banking.**

## The Banking Industry Opportunity:

Banks have a strong vested interest in the new technology gold rush. Their interest will either be driven by the promises of incremental revenues as a result of increased transaction velocity, or a motivation to protect themselves from on-going fraud and the threat of increased regulation. In a study conducted by Ipsos-Insight in January of 2004, it was learned that 42% of consumers have either been a victim, or know a victim, of credit card or on-line fraud. The same study reported that 69% had major concerns with respect to on-line credit card theft and fraudulent use. [36] These concerns have led to a stiff resistance of households to using on-line banking. The TowerGroup reported in June of 2003 that security was the primary concern of households as to why they were not using on-line banking. [37]



Source: TowerGroup, June 2003 – among households not using online banking

# *IT Security – The New Technology Gold Rush*

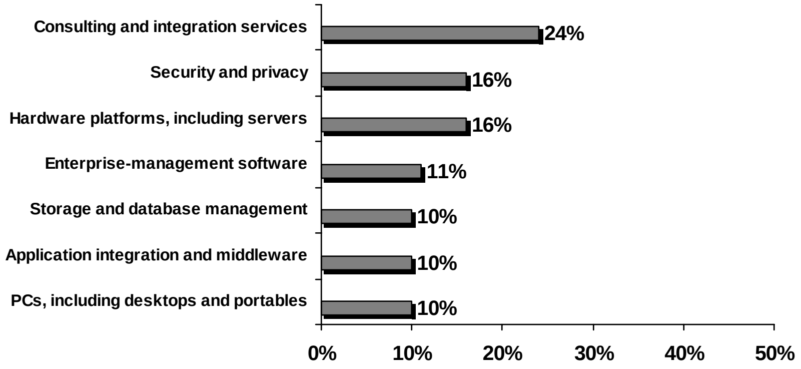
Banks have hoped to use on-line banking as a means of generating incremental revenue on transactions, as well as increased process efficiencies and lower operational costs. Investments in on-line banking infrastructure have been substantial to date, with very little pay off. Those investments are likely to increase as banks look to deploy next generation IT security solutions to bolster infrastructure security in order to entice customers to on-line banking.

**VARBusiness found that 16% of the VARBusiness 500 companies expect to exceed their sales expectations in the area of security and privacy solutions.**

**The Channel Opportunity:**

The new technology gold rush is being actively mined by hundreds of thousands of channel partners through out the world, selling everything from simple virus protection software, to complex enterprise level IT security solutions. The IT security space has ended up being, and should continue to be, a fertile area of opportunity for channel partners. This is largely due to the still "mysterious" nature of IT security to many business owners and IT executives. The recent 2004 RSA conference in San Francisco witnessed a great deal of activity that focused around the simple issue of "tell me what this is all about and what I need to do." As long as there are security threats, combined with gaps in understanding and skills, channel partners should find great success in selling and deploying IT security products, services, and solutions. For this reason, VARBusiness found that 16% of the VARBusiness 500 companies expect to exceed their sales expectations in the area of security and privacy solutions in 2004. In the same study, 24% responded that consulting and integration service revenues were poised to exceed quotas, which revenues are bound to include one or more elements of security. [38]

**Technology Product and Service Areas that VARBusiness 500 Companies Expect to Exceed Sales Expectations (as a % of respondents)**



Source: VARBusiness, July 2003; n=83 executives from the VARBusiness 500

IT security vendors have long since understood the complex nature of security deployments and have continually worked and reworked their channel partner recruiting strategies and programs to address these opportunities. Checkpoint recently recruited 400 new partners in the US that will focus mainly on the small business segment, giving them several thousands of channel partners in the US alone. Competitor Network Associates has an estimated 2,600 US partners in the US today, while Cisco and Symantec are reported to have tens of thousands of channel partners in the US according to *CRN Magazine*. [39]

**IntelliClear expects there to be a tremendous increase in the number of companies contracting for remote network management and monitoring of key elements of the IT infrastructure.**

Another area of opportunity for channel partners will be in the area of security monitoring. IntelliClear expects there to be a tremendous increase in the number of companies contracting for remote network management and monitoring of key elements of the IT infrastructure. Although it may appear "anti-security" to allow a 3rd party to monitor the IT infrastructure, such practices are becoming seriously considered and deployed among mid-size companies today. Vendors who offer these services are going both down and upstream to peddle their remote monitoring services in hopes of gaining greater traction and revenue opportunities. Ernst & Young released the results of a study in August of 2003 among companies WW that reported ISP's and business partners/suppliers were the top two choices (47% and 45% respectively) of groups to be notified in the event of an information security incident. [40] Certainly channel partners of all types will qualify as being business partners/suppliers, while many offer ISP services as well. These monitoring opportunities not only create revenue streams for services, but will also drive new PC and software sales.

Whether channel partners are servicing large enterprise, government, educational, small, medium, or consumers, IT security is providing rich opportunities for revenue across a broad range of products and services.

**Employment Firms and Workforce Opportunities:**

The final area that IntelliClear will examine is the opportunities being created from the new technology gold rush for individuals and firms that supply skilled labor. Up to this time, IntelliClear has focused on the opportunities for companies and channels; however, at the end of the day it will take skilled individuals to drive and execute on these opportunities. As such, resource priorities and a lack of skilled staff were the number two and three most significant obstacles (respectively) to effective IT security WW according to Ernst & Young. [41] Such human resource constraints create serious implementation barriers and are a threat to the IT security opportunity.

# IT Security – The New Technology Gold Rush

With IT security skills in such great demand, and the environment changing so rapidly, solution providers are having to constantly train and hire new individuals to stay on top of evolving regulations and technologies. The average information security specialist in 2003 made just over $75,000 per year according to *Computerworld* in October of 2003, with annual salary increases projected at a healthy 2.3%.[42] With demand so high, and supply so limited, many firms will be leery of training individuals for fear of losing them to the IT security bidding wars for qualified resources.

**The Emmes Group reported in May of 2003 that 47.2% of IT professionals were spending over $50,000 per year on computer/network security consulting services, while 37.6% were spending over $100,000 per year.**

To address their own needs, companies are turning to high priced IT security consultants to fill the missing internal voids. The Emmes Group reported in May of 2003 that 47.2% of IT professionals were spending over $50,000 per year on computer/network security consulting services, while 37.6% were spending over $100,000 per year.[43] Recruiting firms are struggling to keep up with the demand for skilled IT security resources, while professional employee services firms such as ManPower, Adecco, Randstad, Vedior, should be strategizing on how to best capture the low hanging resource fruit in the IT space. The new technology goldrush is creating demand for not only generalized IT security skills, but specialized IT security skills across a broad spectrum of technologies and vertical industries.

**<u>The Future of the Gold Rush – IntelliClear Commentary:</u>**

IntelliClear has sought to examine the IT security space by looking at the size of the market, the drivers and inhibitors of IT security, the key areas of interest, and those who are best positioned to capture the opportunity. IT security is a global opportunity which will require a local focus and a universal perspective. As on going education creates a broader awareness and understanding of IT security, the mystery of IT security will erode and the opportunity will evolve for all those who are mining the golden opportunity.

In the next 6-12 months IntelliClear believes that companies large and small are likely to continue to struggle with the common issues of authentication and verification, email and anti-virus filtering, and firewall implementations. Although these three areas are not considered particularly new, all three can have an enormous impact on a company's perceived security and productivity. Providers of security products and services should focus attention on improving their performance on continuous patch management; management tools that cross product and brand platforms, and integration of point solutions. Besides highlighting the virtues of "increased security," suppliers of IT security products and services (including PC and server OEMs) should create extended value propositions that include the merits of system manageability, lower total cost of ownership, and higher system availability. By doing so, vendors can address not only the functional benefits of their security solutions, but also the emotional, and even self-expressive, benefits of deploying their particular IT security solutions.

**Besides highlighting the virtues of "increased security," suppliers of IT security products and services should create extended value propositions that include the merits of system manageability, lower total cost of ownership, and higher system availability.**

Lastly, there is a myth that most security issues lead back to Microsoft software. Those in the inner circle know that this is far from the truth. The pervasive use of the Microsoft O/S, both on the client and server, make it the logical target for hackers and would-be thieves across the globe. Microsoft has greatly improved its responsiveness to security issues, although it may never be able to match the responsiveness of the Linux environment. Of course, if Linux ever has the opportunity to become as pervasive as Microsoft across millions of homes and organizations, it too will be held hostage to revision and process control management. The industry needs broader consortiums to better understand and deal with a wide variety of security issues – both known and unknown. The time is right to do so, with a slightly more humble Microsoft, and markedly savvier IT security ecosystem.

Let the mining of the golden opportunity continue!

**About IntelliClear:**

IntelliClear is a market research and business consulting firm founded in 2004 under the direction of Eric Shuster, a 24 year IT industry veteran. IntelliClear's mission is to bring clarity to IT market intelligence by delivering results-oriented research, responsive industry experience, and effective data synthesis - leading to confident go-to-market plans. IntelliClear leverages the extensive background of Mr. Shuster, while utilizing its broad network of industry consultants and research partners as part of its operational model to execute projects across a wide variety of research methodologies, markets, and geographies.

## Cited Sources and Notes:

[1] The Building Blocks of Information Security, Ken M. Shaurette, CISSP; Auerebach Publications, 2000

[2] International Data Corporation February 2003

[3] META group, November 2003

[4] SMBs Spent $1.8B on IT Security in 2003; Small Biz Pipeline News, February 24, 2004; AMI-Partners source

[5] INPUT 2003; US Federal Government Spending on IT Products

[6] International Data Corporation (IDC), March 2003 n=280

[7] Deloitte & Touche and IDG Research Services Group, April 2003; n=200

[8] Forrester Research, November 2003; n=818 IT decision makers (based upon average index score)

[9] ARC Research; VARBusiness , August 2003; n=285 medium sized companies (100-999 employees)

[10] SMBs Spent $1.8B on IT Security in 2003; Small Biz Pipeline News, February 24, 2004; AMI-Partners source

[11] Ernst & Young, August 2003; n=1,424 IT executives, multiple responses allowed

[12] Forrester Research, August 2003; n=50 ($1 billion+ in revenues)

[13] CRN Magazine, 2/23/04 (page 26)

[14] Ernst & Young, August 2003; n=1,413 IT executives, multiple responses allowed

[15] CIO Insight, March 2003

[16] Greg Shipley, Network Computing: May 27, 2002

[17] Ernst & Young, July 2003; n=1,425 IT executives

[18] Emmes Group for Stonesoft, May 2003; n=375 IT professionals (RSA 2003 conference attendees)

[19] Aladdin Knowledge Systems, January 2003; n=470, multiple responses allowed

[20] Pointsec Mobile, July 2003

[21] SearchSecurity.com for Rainbow Technologies, April 2003; n=300 IT professionals

[22] ARC Research; VARBusiness, August 2003; n=285 businesses of 100-999 employees

[23] PricewaterhouseCooopers, April 2003

[24] Strategy Analytics, July 2003

[25] Strategy Analytics, July 2003

[26] Yankee Group/Sunbelt Software Inc., April 2003, n=1,000 (numbers may add up to 100% due to rounding

[27] Software Information and Industry Association (SIIA), October 2003

[28] Morgan Stanley, July 2003, n=225 US CIOs

[29] Gartner Dataquest, July 2002 (includes adapters, access points, broadband gateways, and other WLAN equipment

[30] Morgan Stanley, July 2003, n=225 US CIOs

[31] Evans Data, September 2003, n=462 wireless developers

[32] CIO Magazine Tech Poll, December 2003, n=274

[33] PricewaterhouseCoopers, April 2003

[34] Morgan Stanley, July 2003, n=225

IntelliClear
Bringing Clarity to IT Market Intelligence

Clarity Brief

[35] Network World/Research Concepts, LLC, June 2003

[36] Ipsos-Insight, January 2004, n=943

[37] TowerGroup, June 2003 (among households not using on-line banking)

[38] VARBusiness, June 2003, n=83 executives from the VARBusiness 500

[39] CRN Magazine, 2/23/04, page 18

[40] Ernst & Young, August 2003

[41] Ernst & Young, August 2003, n=1,413 IT executives, multiple responses allowed

[42] Computerworld, October 2003 (combination of salary and bonus)

[43] Emmes Group for Stonesoft, May 2003, n=375 RSA Conference Attendees

Clarity Brief

IntelliClear Inc.
12594 Woodmont Drive, Suite 120
Colorado Springs, CO  80921
Phone:  (719) 488-4573
Fax:  (719) 488-4574
newengagements@intelliclear.com